SECURITY ISSUES FOR ALL-OPTICAL NETWORKS

Muriel Medard
Massachusetts Institute of Technology
Lincoln Laboratory

In Response to DoD and commercial demand for networks with increased bandwidth and extensibility, there have been many recent research efforts pursuing the development of all-optical networks. All-optical networks promise THz bandwidth, scalability, extensibility, and interoperability with legacy systems, but possess potential, as yet unstudied, security vulnerabilities. The All-Optical Network Consortium testbed we are currently building, The ONTC Testbed, the NONTC Testbed, as well as IBM's commercial RAINBOW network are examples of advanced, high-performance optical wavelength-division multiplexed (WDM) networks. The imminent deployment and use of these types of networks by a combination of DoD and Commercial users calls for a near-term study of the potential vulnerabilities, and their countermeasures. Certain of the vulnerabilities of all-optical networks are also expected to be present in electro-optical networks, and many of the countermeasures developed for all-optical networks would be directly applicable to the electro-optic counterpart, particularly when specific component vulnerabilities are concerned.

We propose research be initiated to investigate methods of increasing the security of all-optical networks against service denial, eavesdropping, traffic analysis, and unauthorized access at a level equal to or greater than in the current generation of electro-optic networks. Such research would focus on all aspects (or Network Levels) of the network, including components, subsystems, network protocols, network management, network monitoring, etc.

In our view, it is important to create a thorough theoretical understanding of the security of all-optical networks, and to understand the salient hardware characteristics that effect network security. Currently operating all-optical network testbeds, existing engineering implementations of fast networked communications, and both DoD and general societal pressure for technological solutions to privacy and other security concerns combine as an effective motivator to act now.

This work was sponsored by the Defense Advanced Research Projects Agency.